UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/526,935	09/07/2005	Yusuke Hisada	267285US90PCT	7558

22850 7590 01/15/2009

OBLON, SPIVAK, MCCLELLAND MAIER & NEUSTADT, P.C.
1940 DUKE STREET
ALEXANDRIA, VA 22314

EXAMINER	
SU, SARAH	

ART UNIT	PAPER NUMBER
2431	

NOTIFICATION DATE	DELIVERY MODE
01/15/2009	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

patentdocket@oblon.com
oblonpat@oblon.com
jgardner@oblon.com

Office Action Summary	Application No.	Applicant(s)	
	10/526,935	HISADA ET AL.	
	Examiner	Art Unit	
	Sarah Su	2431	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *17 October 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-15* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-15* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *09 September 2008* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

FINAL ACTION

1. Amendment A, received on 9 September 2008 has been entered into record. In this amendment, claims 1, 4-5, 7-9, and 11-14 have been amended. Amendment B, received on 17 October 2008, has been entered into record. In this amendment, claim 11 has been amended.

2. Claims 1-15 are presented for examination.

Response to Arguments

3. Applicant's arguments filed 9 September 2008 have been fully considered but they are not persuasive.

As to claim 1, the applicant argues that Daude does not disclose sending an access control list containing information indicative of a private IP address assigned to the communication unit to a mediating apparatus on the IP network from the VPN gateway unit. The examiner respectfully disagrees. Daude discloses the ACLs are downloaded to each device (i.e. mediating apparatus) in the network (0046, lines 3-4).

As to claims 1 and 9, the applicant argues that Daude does not disclose storing the access control list in the mediating apparatus in correspondence to the VPN gateway unit. The examiner respectfully disagrees. Daude discloses that ACLs reside (i.e. stored) in routers (i.e. mediating apparatus) and that ACLs can be managed for network services using VPNs (0044, lines 2-8). Daude also discloses that gateways are used as interconnection devices for VPNs (Abstract, lines 2-6).

Further, as to claim 1, the applicant argues that Daude does not disclose retrieving, by the mediating apparatus, an IP address of the VPN gateway unit in response to a request from the VPN client unit, acquiring a private address of the corresponding communication unit from the access control list, sending the acquired IP address of the VPN gateway unit and the acquired private IP address to the VPN client unit, sending an IP address of the VPN client unit to the VPN gateway unit, generating mutual authentication information for setting up an authenticated encrypted tunnel between the VPN client unit and the VPN gateway unit, and sending the said mutual authentication information to both of the VPN client unit and the VPN gateway unit. The examiner respectfully disagrees. Daude discloses that a router uses a table lookup to find the address of the destination router (i.e. IP address of the VPN gateway unit) (0029, lines 6-8) and that users are mapped (i.e. private address) from an ACL (0044, lines 4-8). Daude discloses that a portion of a certificate that is transferred may contain an IP address and the identification of the network on which the device is connected to (i.e. VPN gateway unit) (0136, lines 6-9) and another portion may contain the IP destination range (i.e. private IP address) (0138, lines 4-7). Daude discloses that the IP address of the IP device (i.e. VPN client unit) trying to establish a connection is identified (0095, lines 4-6). Daude also discloses that IPsec (i.e. authenticated encrypted tunnel) is used for VPN security (0111, lines 1-2) to connect a device (i.e. VPN client unit) to a gateway (i.e. VPN gateway unit) (0091, lines 1-4; 0108, lines 9-11). Daude also discloses

transferring a certificate (i.e. mutual authentication information) from a certificate authority (0112, lines 1-3).

As to claim 5, the applicant argues that Sutanto does not disclose searching a domain name server to acquire the IP address assigned to the VPN gateway unit. The examiner respectfully disagrees. Sutanto discloses that a request is sent to the DNS (0041, lines 1-2) and that a MAC address is extracted from the response, the MAC address being associated with the gateway IP address (0041, lines 7-11).

Drawings

4. The drawings were received on 9 September 2008. These drawings are acceptable.

Claim Rejections - 35 USC § 103

5. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

6. Claims 1-4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Daude et al. (US 2004/0088542 A1 and Daude hereinafter) in view of Malinen et al. (US 2004/0266420 A1 and Malinen hereinafter).

As to claim 1, Daude discloses a system and method for virtual private network crossovers based on certificates, the system and method having:

(a) sending an access control list containing information indicative of a private IP address assigned to said communication unit to a mediating apparatus (i.e. device) **on said IP network from said VPN gateway unit** (0044, lines 2, 11-13; 0046, lines 3-4)**;**

(b) storing said access control list in said mediating apparatus (i.e. routers) **in correspondence to said VPN gateway unit** (0044, line 2)**;**

(c) retrieving, by said mediating apparatus, an IP address of said VPN gateway unit (i.e. interconnecting device) **in response to a request from said VPN client unit** (0052, lines 6-9)**, acquiring the private IP address of the corresponding communication unit from said access control list, sending the acquired IP address of said VPN gateway unit and the acquired private IP address to said VPN client unit** (0044, lines 4-8)**, sending an IP address of said VPN client unit to said VPN gateway unit** (0095, lines 4-6)**, generating mutual authentication information** (i.e. certificate) **for setting up an authenticated encrypted tunnel between said VPN client unit and said VPN gateway unit** (0108, lines 9-11)**, and sending said mutual authentication information to both of said VPN client unit and said VPN gateway unit** (0096, lines 4-8)**.**

Daude does not disclose:

(d) setting up said authenticated encrypted tunnel between said VPN client unit and said VPN gateway unit by use of said mutual authentication information, and implementing remote access through said encrypted tunnel by use of the private IP address of said communication unit.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Daude, as evidenced by Malinen.

Malinen discloses a system and method for secure mobile connectivity, the system and method having:

(d) setting up said authenticated encrypted tunnel between said VPN client unit and said VPN gateway unit by use of said mutual authentication information, and implementing remote access through said encrypted tunnel by use of the private IP address of said communication unit (0004, lines 4-9; 0042, lines 1-3)**.**

Given the teaching of Malinen, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Daude with the teachings of Malinen by creating an authenticated encrypted tunnel for remote access communications. Malinen recites motivation by disclosing that defining a protocol for an authenticated encrypted tunnel for communications ensures the security of transmitted information packets (0004, lines 1-4). It is obvious that the teachings of Malinen would have improved the teachings of Daude by creating an authenticated encrypted tunnel for communications in order to ensure the security of packets being transmitted.

As to claim 2, Daude discloses:

wherein said access control list contains attribute information about said VPN client unit (0007, lines 5-8).

As to claim 3, Daude discloses:

wherein said step (a) includes a step of encrypting a communication channel between said mediating apparatus and said VPN gateway unit or a VPN gateway management unit having an authority of its management (0023, lines 3-5)**, and sending said access control list from said VPN gateway unit to said mediating apparatus** (0044, line 2, 11-13; 0046, lines 3-4).

As to claim 4, Daude discloses:

wherein said step (b) includes steps of: authenticating said VPN gateway unit by said mediating apparatus (0096, lines 4-8)**;**

storing said access control list for said VPN client unit sent from said VPN gateway unit when the authentication is successful (0044, line 2).

7. Claims 5, 7-8 are rejected under 35 U.S.C. 103(a) as being unpatentable over Daude in view of Malinen as applied to claims 2 and 3 above, and further in view of Sutanto (US 2003/0039240 A1).

As to claim 5, Daude, combined with Malinen, discloses:

wherein said step (c) includes the steps of: (c-0) on receiving a request for retrieval of an IP address assigned to said VPN gateway unit from said VPN client unit, verifying whether said VPN client unit has an authority of access to said VPN gateway unit (0052, lines 4-6)**;**

only when said VPN client unit has said access authority, (c-1) referring to said access control list, and acquiring the private IP address assigned to said communication unit (0044, lines 4-8)**;**

(c-3) generating said mutual authentication information for authentication between said VPN client unit and said VPN gateway unit (0108, lines 9-11)**;**

(c-4) encrypting a first communication channel between said mediating apparatus and said VPN client unit (0023, lines 3-5)**, and sending said mutual authentication information, the IP address of said VPN gateway unit and the private IP address of said communication unit to said VPN client unit** (0044, lines 4-8; 0052, lines 6-9)**;**

(c-5) encrypting a second communication channel between said mediating apparatus and said VPN gateway unit (0023, lines 3-5)**, and sending to said VPN gateway unit said mutual authentication information, an IP address of said VPN client unit and said attribute information about said VPN client unit described in said access control list** (0044, lines 2, 11-13; 0046, lines 3-4; 0052, lines 6-9)**.**

Daude in view of Malinen does not disclose:

(c-2) searching a domain name server to acquire the IP address assigned to said VPN gateway unit.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Daude in view of Malinen, as evidenced by Sutanto.

Sutanto discloses a system and method for accessing an embedded web server on a broadband access terminal, the system and method having:

(c-2) searching a domain name server to acquire the IP address assigned to said VPN gateway unit (0041, lines 1-2, 7-11).

Given the teaching of Sutanto, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Daude in view of Malinen with the teachings of Sutanto by using a domain name server to obtain a device's IP address. Sutanto recites motivation by disclosing that communications can be monitored by identifying a dynamic host configuration protocol packet directed to a user terminal, which can be accomplished with the IP address of a domain name server or gateway (0006, lines 1-4, 10-16). It is obvious that the teachings of Sutanto would have improved the teachings of Daude in view of Malinen by using a domain name server to obtain an IP address so that communications can be monitored.

As to claim 7, Daude in view of Malinen does not disclose:

wherein: letting a domain name server be denoted by DNS, said step (c) includes a step wherein said VPN client unit captures a DNS query transferred from an in-unit application or another VPN client unit, then collates the source address and contents of said query with filtering conditions, and, if they match the conditions, converts said query to a query to said mediating apparatus;

said step (d) includes a step setting/updating tunneling protocol configuration management information on the basis of an answer to said query;

said step (e) includes a step of initializing the tunnel as required, passing the private IP address of the communication unit specified by said mediating unit, as the result of said DNS query, to the application of the query source.

Nonetheless, these features are well known in the art and would have been an obvious modification of the teachings disclosed by Daude in view of Malinen, as evidenced by Sutanto.

Sutanto discloses:

wherein: letting a domain name server be denoted by DNS, said step (c) includes a step wherein said VPN client unit captures a DNS query transferred from an in-unit application or another VPN client unit, then collates the source address (i.e. MAC address) **and contents of said query with filtering conditions, and, if they match the conditions, converts said**

query to a query to said mediating apparatus (i.e. DNS server) (0031, lines 3-13);

said step (d) includes a step setting/updating tunneling protocol configuration management information (i.e. HTTP request) **on the basis of an answer to said query** (0032, lines 14-18);

said step (e) includes a step of initializing the tunnel as required, passing the private IP address of the communication unit specified by said mediating unit, as the result of said DNS query, to the application of the query source (i.e. user terminal) (0031, lines 13-16).

Given the teaching of Sutanto, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Daude in view of Malinen with the teachings of Sutanto by intercepting a DNS query and using the resultant information to create a tunnel. Sutanto recites motivation by disclosing that hijacking a DNS query allows for access to diagnostic web pages (0003, lines 10-11) and that creating communications based on the result allows requests for websites to be sent to the IP address through the gateway (0031, lines 16-18). It is obvious that the teachings of Daude in view of Marlinen would have benefited from the teachings of Sutanto by intercepting DNS queries and creating a communication line accordingly in order to provide for a way to access diagnostic web pages and provide for website requests through a gateway.

As to claim 8, Daude, combined with Malinen and Sutanto, discloses:

wherein, letting simple public key infrastructure be denoted by SPKI, said step (c) includes a step wherein said VPN client unit issues a certificate by an SPKI scheme (0069, lines 2-4; 0081, lines 3-5), **and another VPN client unit having received said certificate** (0069, lines 6-8) **sends to said mediating apparatus a request for retrieval of the IP address assigned to said VPN gateway unit** (0052, lines 6-9). The examiner asserts that the SPKI scheme is another way to perform authentication using public keys and that it would have been obvious to use the SPKI scheme to modify the usage of public keys in the teachings of Daude to obtain the claimed invention.

8. Claim 6 is rejected under 35 U.S.C. 103(a) as being unpatentable over Daude in view of Malinen and Sutanto as applied to claim 5 above, and further in view of Haverinen et al. (US 2004/0208151 A1 and Haverinen hereinafter).

As to claim 6, Daude in view of Malinen, combined with Sutanto, discloses:

wherein, at the time of setting up the encrypted tunnel between said VPN client unit and said VPN gateway unit, said VPN gateway unit performs at least one of (0004, lines 4-9; 0042, lines 1-3)**: a function of determining the private IP address to be given to said VPN client unit on the basis of said attribute information on said VPN client unit sent from said mediating apparatus, and giving the determined private IP address to said VPN client unit; a function of determining a VLAN to be accommodated on the basis of said attribute information about said VPN client unit, a gateway address, an**

internal DNS address, a WINS server address, etc.; a function of changing packet filtering setting of said VPN gateway unit on the basis of said attribute information (i.e. ACL) (0062, lines 8-11) in order to prevent spoofed packets from reaching the VPN gateway or home agent, as recited by Malinen (0062, lines 8-9, 11-13). It is obvious that the teachings of Daude and Sutanto would have benefited from the teachings of Malinen by creating a tunnel that filters spoofed packets in order to prevent the spoofed packets from reaching the gateway or home agent.

Daude in view of Malinen and Sutanto does not disclose:

wherein when the tunnel established between said VPN gateway unit and said VPN client unit is disconnected or no communication has been conducted via said tunnel for a predetermined period of time, said VPN gateway unit performs tunnel cleanup processing, processing for returning the private IP address assigned to said VPN client unit, and restoring the setting of the packet filtering of said VPN gateway unit used for said VPN client unit concerned.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Daude in view of Malinen and Sutanto, as evidenced by Haverinen.

Haverinen discloses a system and method for authentication in a wireless telecommunications system, the system and method having:

wherein when the tunnel established between said VPN gateway unit and said VPN client unit is disconnected or no communication has been conducted via said tunnel for a predetermined period of time, said VPN gateway unit performs tunnel cleanup processing, processing for returning the private IP address assigned to said VPN client unit, and restoring the setting of the packet filtering of said VPN gateway unit used for said VPN client unit concerned (0043, lines 33-41)**.**

Given the teaching of Haverinen, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Daude in view of Malinen and Sutanto with the teachings of Haverinen by restoring the packet filtering when a tunnel becomes unused. Haverinen recites motivation by disclosing that a record of device connections is kept along with packet transfer information for the purposes of billing (0043, lines 41-46), necessitating that authentication be performed regularly to reflect usage. If authentication fails, the device is not allowed access (i.e. original state). The examiner asserts that if authentication is attempted without a connection, the process will fail and the device will no longer be allowed access. It is obvious that the teachings of Daude in view of Malinen and Sutanto would have benefited from the teachings of Haverinen by resetting filtering information if a connection is lost or unused in order allow for the tracking of device connections.

9. Claims 9-15 are rejected under 35 U.S.C. 103(a) as being unpatentable over Daude in view of Sutanto.

As to claim 9, Daude discloses **a system wherein: VPN client units and a VPN gateway unit are connected to the IP network** (100, 110, 120, 160, Figure 1); **communication units** (i.e. component) **are connected to a local area network placed under the management of the VPN gateway unit** (0080, lines 1-4); **and a remote-access VPN by a tunneling protocol is implemented between an arbitrary one of said VPN client units and said VPN gateway unit connected to said IP network and an arbitrary one of said communication units connected to said local area network placed under the management of said VPN gateway unit** (0076, lines 1-3); **said apparatus comprising:**

ACL storage means for storing an access control list, hereinafter referred to as ACL, sent from said VPN gateway unit and containing information indicative of a private IP address assigned to said communication unit (0044, lines 2, 11-13; 0046, lines 3-4);

authentication/access authorization control means for authenticating said VPN client unit and said VPN gateway unit, and for executing access authorization control (0052, lines 4-6);

authentication information generating means for generating mutual authentication information for setting up an authenticated encrypted tunnel between said VPN client unit and said VPN gateway unit (0108, lines 9-11);

communication means for sending the IP address of said VPN gateway unit, the private IP address of said communication unit and said mutual authentication information to said VPN client unit (0044, lines 4-8), **and for sending the IP address of said VPN client unit and said mutual authentication information to said VPN gateway unit** (0095, lines 4-6).

Daude does not disclose:

IP address acquiring means for referring to said access control list to acquire the private IP address assigned to said communication unit, and for searching a domain name server to acquire an IP address assigned to said VPN gateway unit.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Daude, as evidenced by Sutanto.

Sutanto discloses:

IP address acquiring means for referring to said access control list to acquire the private IP address assigned to said communication unit (0003, lines 4-6, 15-16), **and for searching a domain name server to acquire an IP address assigned to said VPN gateway unit** (0006, lines 7-9).

Given the teaching of Sutanto, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Daude with the teachings of Sutanto by retrieving an IP address of a client from an access control unit and an IP address of a gateway from a domain name server. Sutanto recites motivation by disclosing that retrieving an IP address from a

server (i.e. list) allows connection when the WAN link is not available when the broadband access terminal is powered up (0003, lines 10-16). Please also refer to the motivation as recited above in respect to claim 5 as to why it is obvious to apply the teachings of Sutanto to the teachings of Daude.

As to claim 10, Daude discloses:

wherein said communication means includes encryption means for encrypting communications between said mediating apparatus and said VPN client unit, and communications between said mediating apparatus and said VPN gateway unit (0023, lines 3-5).

As to claims 11 and 12, Daude discloses:

wherein said authentication/access authorization control means is configured to: authenticates said VPN client unit (0096, lines 4-8);

causes said mutual authentication information generating means to generate said mutual authentication information (0108, lines 9-11);

causes said communication means to send the acquired IP address, the private IP address assigned to said communication unit, and said generated mutual authentication information to said VPN client unit (0044, lines 4-8).

Daude does not disclose:

only when the authentication is successful, causes said IP address acquiring means to query the domain name server about the IP address assigned to said VPN gateway unit and acquire said IP address.

Nonetheless, this feature is well known in the art and would have been an obvious modification of the teachings disclosed by Daude, as evidenced by Sutanto.

Sutanto discloses:

only when the authentication is successful, causes said IP address acquiring means to query the domain name server about the IP address assigned to said VPN gateway unit and acquire said IP address (0041, lines 1-2, 7-11)

Given the teaching of Sutanto, a person having ordinary skill in the art at the time of the invention would have readily recognized the desirability and advantages of modifying the teachings of Daude with the teachings of Sutanto by using a domain name server to retrieve the IP address of the gateway. Please refer to the motivation recited above in respect to claim 5 as to why it is obvious to apply the teachings of Sutanto to the teachings of Daude.

As to claim 13, Daude discloses:

wherein said authentication/access authority control means is configured to: authenticate said VPN gateway unit (0096, lines 4-8);

only when the authentication is successful, causes said communication means to send the IP address assigned to said VPN client

unit and said mutual authentication information to said VPN gateway unit (0096, lines 4-8).

As to claim 14, Daude discloses:

wherein said authentication/access authorization control means is configured to authenticate said VPN client unit and said VPN gateway unit by an SPKI (Simple Public Key Infrastructure) scheme, and/or executes access authorization control (0052, lines 4-6; 0081, lines 3-5). The examiner asserts that the SPKI scheme is another way to perform authentication using public keys and that it would have been obvious to use the SPKI scheme to modify the usage of public keys in the teachings of Daude to obtain the claimed invention.

As to claim 15, Daude discloses:

wherein said authentication/access authorization control means authenticates said VPN client unit and said VPN gateway unit by a PKI (Public Key Infrastructure) scheme (0052, lines 4-6; 0081, lines 3-5). The examiner asserts that the PKI scheme is another way to perform authentication using public keys and that it would have been obvious to use the PKI scheme to modify the usage of public keys in the teachings of Daude to obtain the claimed invention.

Conclusion

10. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Sarah Su whose telephone number is (571) 270-3835.

The examiner can normally be reached on Monday through Friday 7:30AM-5:00PM EST..

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Sarah Su/
Examiner, Art Unit 2431

/Christopher A. Revak/

Primary Examiner, Art Unit 2431